JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 11316542
(43)Date of publication of application: 16.11.1999

(51)Int.Cl.

G09C 1/00
G09C 1/00
G09C 1/00
H04L 9/32

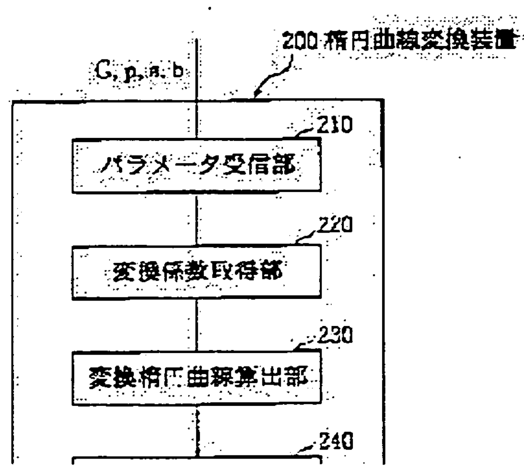
(21)Application number: 11056592	(71)Applicant:	MATSUSHITA ELECTRIC IND CO LTD	
(22)Date of filing: 04.03.1999	(72)Inventor:	MIYAJI MITSUKO	

(30)Priority
Priority number: 10 53204 Priority date: 05.03.1998 Priority country: JP

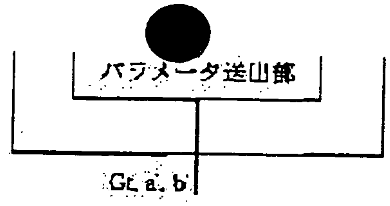
(54) ELLIPTIC CURVE CONVERTING DEVICE, AND DEVICE AND SYSTEM FOR UTILIZATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an elliptic curve converting device which converts an elliptic curve selected optionally as a safe elliptic curve suitable for ciphering into an elliptic curve having safety equivalent to that of the said elliptic curve and capable of decreasing the calculation quantity.
SOLUTION: Relating to this converting device 200, a conversion coefficient acquisition part 220 uses parameters (a) and (b) and an element G of a received elliptic curve E to obtain a conversion coefficient (t) as an element on a finite body GF(p) so that t4 × a(mod p) is 32 bits. A converted



elliptic curve calculation part 230 calculates parameters a' and b' of an elliptic curve Et:y'2=x'3+a' × x'+b' constituted on the finite body GF (p) to calculate an element Gt on the elliptic curve Et. A parameter sending-out part 240 send out the calculated parameters a' and b' and element Gt(xt0, yt0).



LEGAL STATUS

[Date of request for examination] 13.09.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

E 5353

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報(Ａ)　(11)特許出願公開番号

特開平11－316542

(43)公開日　平成11年(1999)11月16日

(51)Int.Cl.⁶		識別記号	FI		
Ｇ０９Ｃ	1/00	６２０	Ｇ０９Ｃ	1/00	６２０Ｚ
					６２０Ａ
		６４０			６４０Ｂ
		６５０			６５０Ｚ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ

審査請求　未請求　請求項の数12　ＯＬ　（全 17 頁）

(21)出願番号　特願平11－56592

(22)出願日　平成11年(1999)３月４日

(31)優先権主張番号　特願平10－53204

(32)優先日　平10(1998)３月５日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　宮地　充子
石川県能美郡辰口町旭台一丁目50番Ｄ－34号

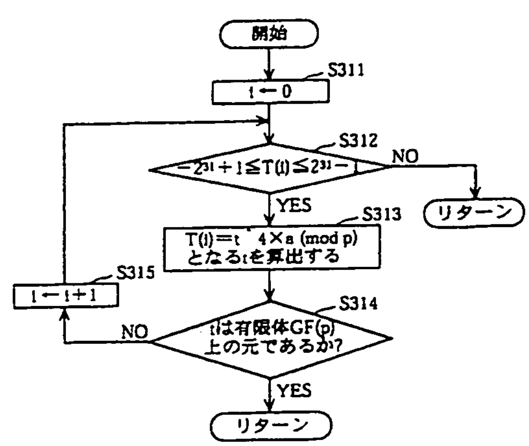
(74)代理人　弁理士　中島　司朗　（外１名）

(54)【発明の名称】　楕円曲線変換装置、利用装置及び利用システム

(57)【要約】

【課題】　本発明は、暗号に適した安全な楕円曲線として任意に選択された楕円曲線を、この楕円曲線と等価な安全性を有し、計算量を削減できる楕円曲線に変換する楕円曲線変換装置を提供することを目的とする。

【解決手段】　受信した楕円曲線Ｅのパラメータａ、ｂと元Ｇとを用いて、変換係数取得部２２０は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が３２ビット以下になるように、有限体ＧＦ（ｐ）上の元である変換係数ｔを取得し、変換楕円曲線算出部２３０は、有限体ＧＦ（ｐ）上に構成される楕円曲線Ｅｔ：ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’のパラメータａ’、ｂ’を算出し、楕円曲線Ｅｔ上の元Ｇｔを算出し、パラメータ送出部２４０は、前記算出されたパラメータａ’、ｂ’と、元Ｇｔ（ｘｔ０，ｙｔ０）とを外部へ送出する。



【特許請求の範囲】

【請求項１】　１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置であって、
外部から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポンイトとしての元Ｇとを受信する手段であって、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表される受信手段と、
有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得する手段であって、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満たす変換係数取得手段と、
前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイント元Ｇｔとを算出する手段であって、
ａ’＝ａ×ｔ＾４、
ｂ’＝ｂ×ｔ＾６、
ｘｔ０＝ｔ＾２×ｘ０、
ｙｔ０＝ｔ＾３×ｙ０、
楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値である楕円曲線算出手段と、
前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを外部へ出力する出力手段とを備えることを特徴とする楕円曲線変換装置。

【請求項２】　ｐは、１６０ビットの素数であり、
前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が３２ビット以下の数になる、という条件を満たす変換係数ｔを取得することを特徴とする請求項１記載の楕円曲線変換装置。

【請求項３】　前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が－３となる、という条件を満たす変換係数ｔを取得することを特徴とする請求項１記載の楕円曲線変換装置。

【請求項４】　前記変換係数取得手段は、変数Ｔとして、初期値を－３とし、初期値以外の値については、桁数の小さい値から大きい値へ順に取ることと、
Ｔ＝ｔ＾４×ａ　（ｍｏｄ　ｐ）
という条件を満たすかどうかを判定することとを繰り返すことにより、変換係数ｔを取得することを特徴とする請求項１記載の楕円曲線変換装置。

【請求項５】　１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置と、生成された楕円曲線Ｅｔを利用する利用装置とからなる楕円曲線利用システムであって、
前記利用装置は、第１出力手段と第１受信手段と利用手段とを備え、前記楕円曲線変換装置は、第２受信手段と変換係数取得手段と楕円曲線算出手段と第２出力手段とを備え、
前記第１出力手段は、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを前記楕円曲線変換装置へ出力し、
ここで、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、
ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、
元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、
前記第２受信手段は、前記利用装置から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、元Ｇとを受信し、
前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、
ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、
前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出し、
ａ’＝ａ×ｔ＾４、
ｂ’＝ｂ×ｔ＾６、
ｘｔ０＝ｔ＾２×ｘ０、
ｙｔ０＝ｔ＾３×ｙ０、
ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、
ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、
ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値であり、
前記第２出力手段は、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを前記利用装置へ出力し、
前記第１受信手段は、前記出力されたパラメータａ’及びｂ’と、元Ｇｔとを受信し、
前記利用手段は、素数ｐと、前記受信したパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポイントとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行うことを特徴とする楕円曲線利用システム。

【請求項６】　ｐは、１６０ビットの素数であり、
前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が３２ビット以下の数になる、という条件を満たす変換係数ｔを取得することを特徴とする請求項５記載の楕円曲線利用システム。

【請求項７】　前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が－３となる、という条件を満たす変換係数ｔを取得することを特徴とする請求項５記載の楕円

曲線利用システム。

【請求項８】 前記変換係数取得手段は、変数Ｔとして、初期値を－３とし、初期値以外の値については、桁数の小さい値から大きい値へ順に取ることと、

Ｔ＝ｔ＾４×ａ （ｍｏｄ ｐ）

という条件を満たすかどうかを判定することとを繰り返すことにより、変換係数ｔを取得することを特徴とする請求項５記載の楕円曲線利用システム。

【請求項９】 第２受信手段と変換係数取得手段と楕円曲線算出手段と第２出力手段とを備え、１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置から、前記生成された楕円曲線Ｅｔを受信して利用する利用装置であって、

前記利用装置は、第１出力手段と第１受信手段と利用手段とを備え、

前記第１出力手段は、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを前記楕円曲線変換装置へ出力し、

ここで、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、

ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、

元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、

前記第２受信手段は、前記利用装置から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、元Ｇとを受信し、

前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、

ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ （ｍｏｄ ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、

前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、元Ｇｔとを算出し、

ａ’＝ａ×ｔ＾４、

ｂ’＝ｂ×ｔ＾６、

ｘｔ０＝ｔ＾２×ｘ０、

ｙｔ０＝ｔ＾３×ｙ０、

ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、

ｙ’＾２ ＝ ｘ’＾３ ＋ａ’×ｘ’＋ｂ’で表され、

ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値であり、

前記第２出力手段は、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを前記利用装置へ出力し、

前記第１受信手段は、前記出力されたパラメータａ’及びｂ’と、元Ｇｔとを受信し、

前記利用手段は、素数ｐと、前記受信したパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポンイトとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行うことを特徴とする利用装置。

【請求項１０】 １つの楕円曲線Ｅを変換して生成された楕円曲線Ｅｔを利用する利用装置であって、

前記利用装置は、

楕円曲線Ｅｔのパラメータａ’及びｂ’と、ベースポイントとしての元Ｇｔとを記憶している記憶手段と、

ｐと、前記記憶しているパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポイントとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行う利用手段とを備え、

ここで、パラメータａ’及びｂ’と、元Ｇｔとは楕円曲線変換装置により生成され、

前記楕円曲線変換装置は、変換係数取得手段、楕円曲線算出手段を備え、

ｐは素数であり、

楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、

ベースポンイトとしての元Ｇが、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、

前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ （ｍｏｄ ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、

前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出し、

ａ’＝ａ×ｔ＾４、

ｂ’＝ｂ×ｔ＾６、

ｘｔ０＝ｔ＾２×ｘ０、

ｙｔ０＝ｔ＾３×ｙ０、

ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２ ＝ ｘ’＾３ ＋ａ’×ｘ’＋ｂ’で表され、

ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値であることを特徴とする利用装置。

【請求項１１】 １つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換方法であって、

外部から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポンイトとしての元Ｇとを受信するステップであって、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表される受信ステップと、

有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得するス

テップであって、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満たす変換係数算出ステップと、
前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出するステップであって、
ａ’＝ａ×ｔ＾４、
ｂ’＝ｂ×ｔ＾６、
ｘｔ０＝ｔ＾２×ｘ０、
ｙｔ０＝ｔ＾３×ｙ０、
楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値である楕円曲線算出ステップと、
前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを外部へ出力する出力ステップとを含むことを特徴とする楕円曲線変換方法。

【請求項１２】　１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記プログラムは、
外部から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを受信するステップであって、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表される受信ステップと、
有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得するステップであって、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満たす変換係数算出ステップと、
前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出するステップであって、
ａ’＝ａ×ｔ＾４、
ｂ’＝ｂ×ｔ＾６、
ｘｔ０＝ｔ＾２×ｘ０、
ｙｔ０＝ｔ＾３×ｙ０、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値である楕円曲線算出ステップと、
前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを外部へ出力する出力ステップとを含むことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は情報セキュリティ技術としての暗号技術に関し、特に、楕円曲線を用いて実現する暗号・復号技術、デジタル署名・検証技術及び鍵共有技術に関する。

【０００２】

【従来の技術】１．公開鍵暗号
近年、コンピュータ技術と通信技術とに基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式又はデジタル署名方式が用いられている。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明する通信方式である。

【０００３】これらの秘密通信方式又はデジタル署名方式には公開鍵暗号とよばれる暗号方式が用いられる。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。公開鍵暗号を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。

【０００４】この公開鍵暗号の安全性の根拠として離散対数問題が用いられる。離散対数問題には、代表的なものとして、有限体上定義されるもの及び楕円曲線上定義されるものがある。なお、離散対数問題については、ニイルコブリッツ著　”ア　コウス　イン　ナンバア　セオリイ　アンド　クリプトグラヒイ”(Neal Koblitz, ”A Course in Number theory and Cryptography”, Springer-Verlag,1987)に詳しく述べられている。

２．楕円曲線上の離散対数問題
楕円曲線上の離散対数問題について、以下に述べる。

【０００５】楕円曲線上の離散対数問題とは、Ｅ（ＧＦ（ｐ））を有限体ＧＦ（ｐ）上で定義された楕円曲線とし、楕円曲線Ｅの位数が大きな素数で割り切れる場合に、楕円曲線Ｅに含まれる元Ｇをベースポイントとする。このとき、楕円曲線Ｅに含まれる与えられた元Ｙに対して、

（式１）　Ｙ＝ｘ＊Ｇ

となる整数ｘが存在するならば、ｘを求めよ、という問題である。

【０００６】ここで、ｐは素数、ＧＦ（ｐ）はｐ個の元を持つ有限体である。また、この明細書において、記号＊は、楕円曲線に含まれる元を複数回加算する演算を示し、ｘ＊Ｇは、次式に示すように、楕円曲線に含まれる元Ｇをｘ回加算することを意味する。

ｘ＊Ｇ＝Ｇ＋Ｇ＋Ｇ＋・・・＋Ｇ

離散対数問題を公開鍵暗号の安全性の根拠とするのは、多くの元を有する有限体ＧＦ（ｐ）に対して、上記問題は極めて難しいからである。

３．楕円曲線上の離散対数問題を応用したエルガマル署

名
以下に、上記楕円曲線上の離散対数問題を応用したエルガマル署名によるデジタル署名方式について、図１を用いて、説明する。
【０００７】この図は、上記エルガマル署名によるデジタル署名方式の手順を示すシーケンス図である。ユーザＡ１１０、管理センタ１２０及びユーザＢ１３０は、ネットワークで接続されている。ｐを素数、有限体ＧＦ（ｐ）上の楕円曲線をＥとする。Ｅのベースポイントを Ｇとし、Ｅの位数をｑとする。つまり、ｑは、
（式２）　ｑ＊Ｇ＝０
を満たす最小の正整数である。
【０００８】なお、ｘ座標、ｙ座標ともに∞である（∞、∞）を無限遠点といい、０で表す。この０は、楕円曲線を群とみたときに、無限遠点が加算における「零元」の役割を果たす。
（１）管理センタ１２０による公開鍵の生成
管理センタ１２０は、予め通知されているユーザＡ１１０の秘密鍵ｘＡを用いて、式３に従って、ユーザＡ１１０の公開鍵ＹＡを生成する（ステップＳ１４１～Ｓ１４２）。
（式３）　ＹＡ＝ｘＡ＊Ｇ　＊
＊その後、管理センタ１２０は、素数ｐ、楕円曲線Ｅ及びベースポイントＧをシステムパラメータとして公開し、また、他のユーザＢ１３０にユーザＡ１１０の公開鍵ＹＡを公開する（ステップＳ１４３～Ｓ１４４）。
【０００９】（２）ユーザＡ１１０による署名生成
ユーザＡ１１０は、乱数ｋを生成する（ステップＳ１４５）。次に、ユーザＡ１１０は、
（式４）　Ｒ１＝（ｒｘ，ｒｙ）＝ｋ＊Ｇ
を計算し（ステップＳ１４６）、
（式５）　ｓ×ｋ＝ｍ＋ｒｘ×ｘＡ　（ｍｏｄ　ｑ）
から、ｓを計算する（ステップＳ１４７）。ここで、ｍは、ユーザＡ１１０がユーザＢ１３０へ送信するメッセージである。
【００１０】さらに、ユーザＡ１１０は、得られた（Ｒ１、ｓ）を署名としてメッセージｍとともに、ユーザＢ１３０へ送信する（ステップＳ１４８）。
（３）ユーザＢ１３０による署名検証
ユーザＢ１３０は、
（式６）　ｓ＊Ｒ１＝ｍ＊Ｇ＋ｒｘ＊ＹＡ
が成立するかどうか判定することにより、送信者であるユーザＡ１１０の身元を確認する（ステップＳ１４９）。これは、

（式７）　ｓ＊Ｒ１＝｛（（ｍ＋ｒｘ×ｘＡ）／ｋ）×ｋ｝＊Ｇ
＝（ｍ＋ｒｘ×ｘＡ）＊Ｇ
＝ｍ＊Ｇ＋（ｒｘ×ｘＡ）＊Ｇ
＝ｍ＊Ｇ＋ｒｘ＊ＹＡ

となることから明らかであるである。
４．楕円曲線上の点の加算、２倍算の演算による計算量
上記に示した楕円曲線上の離散対数問題を応用したエルガマル署名によるデジタル署名方式における公開鍵の生成、署名生成、署名検証のそれぞれにおいて、楕円曲線上の点の冪倍の演算の計算が行われる。例えば、式３に示す「ｘＡ＊Ｇ」、式4に示す「ｋ＊Ｇ」、式６に示す「ｓ＊Ｒ１」、「ｍ＊Ｇ」、「ｒｘ＊ＹＡ」は、楕円曲線上の点の冪倍の演算である。
【００１１】楕円曲線の演算公式については、"Efficient elliptic curve exponentiation" (Miyaji, Ono, and Cohen著、Advances in cryptology-proceedings of ICICS'97, Lecture notes incomputer science, 1997, Springer-verlag, 282-290.) に詳しく説明されている。
【００１２】楕円曲線の演算公式について、以下に説明する。楕円曲線の方程式をｙ＾２　＝　ｘ＾３　＋ａ×ｘ＋ｂ　とし、任意の点Ｐの座標を（ｘ１，ｙ１）とし、任意の点Ｑの座標を（ｘ２，ｙ２）とする。ここで、Ｒ＝Ｐ＋Ｑで定まる点Ｒの座標を（ｘ３，ｙ３）とする。
【００１３】なお、この明細書において、記号＾は、冪乗の演算を示し、例えば、２＾３は、２×２×２を意味する。Ｐ≠Ｑの場合、Ｒ＝Ｐ＋Ｑは、加算の演算となる。加算の公式を以下に示す。
ｘ３＝｛（ｙ２－ｙ１）／（ｘ２－ｘ１）｝＾２－ｘ１－ｘ２
ｙ３＝｛（ｙ２－ｙ１）／（ｘ２－ｘ１）｝（ｘ１－ｘ３）－ｙ１
Ｐ＝Ｑの場合、Ｒ＝Ｐ＋Ｑ＝Ｐ＋Ｐ＝２×Ｐとなり、Ｒ＝Ｐ＋Ｑは、２倍算の演算となる。２倍算の公式を以下に示す。
【００１４】
ｘ３＝｛（３ｘ１＾２＋ａ）／２ｙ１｝＾２－２ｘ１
ｙ３＝｛（３ｘ１＾２＋ａ）／２ｙ１｝（ｘ１－ｘ３）－ｙ１
なお、上記演算は、楕円曲線が定義される有限体上での演算である。上記に示すように、２項組座標であるアフィン座標、すなわち今まで述べてきた座標において、楕円曲線上の加算演算を行う場合に、楕円曲線上の加算１回につき、１回の有限体上の逆数計算が必要となる。一般に、有限体上の逆数計算は、有限体上での乗算計算と比較して、１０倍程度の計算量を必要とする。
【００１５】そこで、計算量を削減することを目的として、射影座標と呼ばれる３項組の座標が用いられる。射影座標とは、３項組Ｘ、Ｙ、Ｚからなる座標のことであって、座標（Ｘ，Ｙ，Ｚ）と座標（Ｘ'，Ｙ'，Ｚ'）とに対して、ある数ｎが存在して、Ｘ'＝ｎＸ、Ｙ'＝

nY、Z'＝nZなる関係があるならば、(X，Y，Z)＝(X'，Y'，Z')とするものである。

【0016】アフィン座標(x，y)と射影座標(X，Y，Z)とは、

(x，y)　→　(x，y，1)

(X，Y，Z)→　(X／Y，Y／Z)　(Z≠0のとき)

なる関係で、互いに対応している。ここで、記号→は、次に示す意味で用いている。集合S1の任意の元に、集合S2の一つの元が対応するとき、S1→S2と表記する。

【0017】以下、楕円曲線の演算は、すべて、射影座標で行われるものとする。次に、射影座標上の楕円曲線の加算公式、2倍公式について説明する。これらの公式は、もちろん、前に述べたアフィン座標における加算公式、2倍公式と整合性のあるものである。冪倍の演算は、楕円曲線上の点の加算、2倍算の演算の繰り返しによって実現できる。この冪倍の演算のうち、加算の計算量は、楕円曲線のパラメータに依存しないが、2倍算の計算量は、楕円曲線のパラメータに依存する。

【0018】ここでは、pを160ビットの素数とし、有限体GF(p)上の楕円曲線をE：$y^2 = x^3 + ax + b$ とし、楕円曲線E上の元P、Qをそれぞれ、P＝(X1，Y1，Z1)、　Q＝(X2，Y2，Z2)で表すとき、

R＝(X3，Y3，Z3)＝P＋Q

を以下のようにして、求める。

【0019】(i) P≠Qの場合

この場合、加算の演算となる。

(step 1-1)　中間値の計算

以下を計算する。

(式8)　$U1 = X1 \times Z2^2$

(式9)　$U2 = X2 \times Z1^2$

(式10)　$S1 = Y1 \times Z2^3$

(式11)　$S2 = Y2 \times Z1^3$

(式12)　$H = U2 - U1$

(式13)　$r = S2 - S1$

(step 1-2)　R＝(X3，Y3，Z3)の計算

以下を計算する。

(式14)　$X3 = -H^3 - 2 \times U1 \times H^2 + r^2$

(式15)　$Y3 = -S1 \times H^3 + r \times (U1 \times H^2 - X3)$

(式16)　$Z3 = Z1 \times Z2 \times H$

(ii) P＝Qの場合(すなわち、R＝2P)

この場合、2倍算の演算となる。

【0020】(step 2-1)　中間値の計算

以下を計算する。

(式17)　$S = 4 \times X1 \times Y1^2$

(式18)　$M = 3 \times X1^2 + a \times Z1^4$

(式19)　$T = -2 \times S + M^2$

(step 2-2)　R＝(X3，Y3，Z3)の計算

以下を計算する。

(式20)　$X3 = T$

(式21)　$Y3 = -8 \times Y1^4 + M \times (S - T)$

(式22)　$Z3 = 2 \times Y1 \times Z1$

次に、楕円曲線の加算、2倍算を行う場合の計算量について説明する。ここで、有限体GF(p)上の1回の乗算による計算量を1Mul、1回の2乗算による計算量を1Sqで表す。なお、一般のマイクロプロセッサにおいては、1Sq≒0.8Mulである。

【0021】上記の例によると、P≠Qの場合に示されている楕円曲線上の加算の計算量は、式8～式16において、乗算の回数及び2乗算の回数をカウントすることにより得られ、12Mul＋4Sqである。これは、式8、9、10、11、14、15、16における加算の計算量は、それぞれ、1Mul＋1Sq、1Mul＋1Sq、2Mul、2Mul、2Mul＋2Sq、2Mul、2Mulであることから明らかである。

【0022】また、上記の例によると、P＝Qの場合に示されている楕円曲線上の2倍算の計算量は、式17～式22において、乗算の回数及び2乗算の回数をカウントすることにより得られ、4Mul＋6Sqである。これは、式17、18、19、21、22における2倍算の計算量は、それぞれ、1Mul＋1Sq、1Mul＋3Sq、1Sq、1Mul＋1Sq、1Mulであることから明らかである。

【0023】なお、上記回数のカウントにおいて、例えば、式14の H^3 については、

$H^3 = H^2 \times H$

と展開できるので、H^3 の計算量は、1Mul＋1Sqとし、式18の $Z1^4$ については、

$Z1^4 = (Z1^2)^2$

と展開できるので、$Z1^4$ の計算量は、2Sqとする。

【0024】また、式14の H^2 については、前述の H^3 の計算のプロセスにおいて、H^2 が算出されているので、H^2 の計算量は再度カウントしない。また、乗算の回数のカウントの際、ある値に小さい値を乗じて行われる乗算の回数は、カウントしない。その理由を以下に説明する。ここで言う小さい値とは、式8～式22において、乗算の対象となる小さい固定値であり、具体的には、2、3、4、8などの値である。これらの値は、多くとも4ビットの2進数で表現できる。一方、その他の変数は、通常、160ビットの値を有している。

【0025】一般に、マイクロプロセッサにおいて、乗数と被乗数との乗算は、被乗数のシフトと加算の繰り返しにより行われる。すなわち、2進数で表現される乗数の各ビット毎に、このビットが1であるならば、2進数

で表現される被乗数の最下位ビットが、このビットの存在する位置に一致するように、被乗数をシフトして、1つのビット列を得る。乗数の全ビットについて、このようにして得られた少なくとも1つのビット列をすべて加算する。

【0026】例えば、160ビットの乗数と160ビットの被乗数との乗算においては、160ビットの被乗数を160回シフトし、160個のビット列を得、得られた160個のビット列を加算する。一方、4ビットの乗数と160ビットの被乗数との乗算においては、160ビットの被乗数を4回シフトし、4個のビット列を得、得られた4個のビット列を加算する。

【0027】乗算は、上記に示すようにして行われるので、乗算がある値に小さい値を乗じて行われる場合には、前記繰り返しの回数が少なくなる。従って、その計算量は少ないと見なせるので、乗算の回数にカウントしない。以上説明したように、楕円曲線の2倍算を行う場＊合において、式18には、楕円曲線のパラメータaが含まれている。このパラメータaの値として、例えば、小さい値を採用すると、楕円曲線上の2倍算の計算量は、1Mul分削減でき、3Mul＋6Sqとなる。なお、加算に関しては、楕円曲線のパラメータを変化させても、計算量は変わらない。

5．暗号に適した楕円曲線の選択

次に暗号に適した楕円曲線を選択する方法について説明する。なお、その詳細については、「IEEE P1363 Working draft」（1997年2月6日、IEEE発行）に詳しく書かれている。

【0028】暗号に適した楕円曲線は、以下のステップを繰り返すことにより得られる。

(step 1) 任意の楕円曲線の選択

有限体GF（p）上の任意のパラメータa、bを選ぶ。ここで、a、bは、式23を満たし、pは素数である。

（式23）　4×a＾3＋27×b＾2　≠0　（mod　p）

選択されたa、bを用いて、楕円曲線をE：　y＾2　＝　x＾3　＋a×x＋b　とする。

【0029】(step 2) 暗号に適した楕円曲線であるかどうかを判定楕円曲線Eの元の個数＃E（GF（p））を計算し、

（条件1）　＃E（GF（p））が大きな素数で割り切れ、かつ、

（条件2）　＃E（GF（p））－（p＋1）　≠　0，－1である場合に、楕円曲線Eを採用する。条件1又は条件2を満たさない場合は、楕円曲線Eを棄却し、step 1に戻って、再度、任意の楕円曲線の選択と、判定とを繰り返す。

【0030】

【発明が解決しようとする課題】上記に説明したように、楕円曲線のパラメータaとして固定的に小さい値を選択すると、楕円曲線の冪倍の演算において計算量を削減できるものの、パラメータを予め固定的に取ることにより、暗号に適した安全な楕円曲線を選択しにくいという問題点がある。

【0031】また逆に、上記に説明した楕円曲線の選択方法を用いて、暗号に適した安全な楕円曲線を選択すると、楕円曲線のパラメータaとして小さい値を選択できるとは限らず、計算量を削減できないという問題点がある。このように、暗号に適した安全な楕円曲線を選択し、その楕円曲線での演算量を削減するためには、相互に矛盾し対立する問題点を有する。

【0032】本発明は、上記に示す問題点を解決し、暗号に適した安全な楕円曲線として任意に選択された楕円曲線を、この楕円曲線と等価な安全性を有し、かつ、計算量を削減できる楕円曲線に変換する楕円曲線変換装置、楕円曲線変換方法、及び楕円曲線変換プログラムを記録している記録媒体を提供することを目的とする。また、これにより安全でかつ高速に演算ができる暗号装置、復号装置、デジタル署名装置、デジタル署名検証装置、鍵共有装置などの利用装置及び前記利用装置と前記楕円曲線変換装置とから構成される利用システムを提供することを目的とする。

【0033】

【課題を解決するための手段】上記の問題点を解決するために、本発明は、1つの楕円曲線Eを変換して他の1つの楕円曲線Etを生成する楕円曲線変換装置であって、外部から、素数pと、楕円曲線Eのパラメータa及びパラメータbと、ベースポンイトとしての元Gとを受信する手段であって、楕円曲線Eは、有限体GF（p）上で定義され、y＾2＝x＾3＋ax＋bで表され、元Gは、楕円曲線E上に存在し、G＝（x0，y0）で表される受信手段と、有限体GF（p）上に存在する変換係数tを取得する手段であって、変換係数tは、t≠0であり、かつ、t＾4×a　（mod　p）は、素数pと比較して桁数が小さい、という条件を満たす変換係数取得手段と、前記取得された変換係数tを用いて、次式により、楕円曲線Etのパラメータa'及びb'と、新たなベースポイント元Gtとを算出する手段であって、a'＝a×t＾4、b'＝b×t＾6、xt0＝t＾2×x0、yt0＝t＾3×y0、楕円曲線Etは、有限体GF（p）上で定義され、y'＾2　＝　x'＾3　＋a'×x'＋b'で表され、xt0、yt0は、それぞれ元Gtのx座標値、y座標値である楕円曲線算出手段と、前記算出されたパラメータa'及びb'と、元Gtとを外部へ出力する出力手段とを備えることを特徴とする。

【0034】ここで、pは、160ビットの素数であり、前記変換係数取得手段は、t＾4×a　（mod　p）が32ビット以下の数になる、という条件を満たす

変換係数ｔを取得するように構成してもよい。ここで、前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が－３となる、という条件を満たす変換係数ｔを取得するように構成してもよい。

【００３５】ここで、前記変換係数取得手段は、変数Ｔとして、初期値を－３とし、初期値以外の値については、桁数の小さい値から大きい値へ順に取ることと、Ｔ＝ｔ＾４×ａ　（ｍｏｄ　ｐ）という条件を満たすかどうかを判定することとを繰り返すことにより、変換係数ｔを取得するように構成してもよい。また、本発明は、１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置と、生成された楕円曲線Ｅｔを利用する利用装置とからなる楕円曲線利用システムであって、前記利用装置は、第１出力手段と第１受信手段と利用手段とを備え、前記楕円曲線変換装置は、第２受信手段と変換係数取得手段と楕円曲線算出手段と第２出力手段とを備え、前記第１出力手段は、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを前記楕円曲線変換装置へ出力し、ここで、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、前記第２受信手段は、前記利用装置から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、元Ｇとを受信し、前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出し、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値であり、前記第２出力手段は、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを前記利用装置へ出力し、前記第１受信手段は、前記出力されたパラメータａ’及びｂ’と、元Ｇｔとを受信し、前記利用手段は、素数ｐと、前記受信したパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポイントとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行うことを特徴とする。

【００３６】また、本発明は、第２受信手段と変換係数取得手段と楕円曲線算出手段と第２出力手段とを備え、１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置から、前記生成された楕円曲線Ｅｔを受信して利用する利用装置であって、前記利用装置は、第１出力手段と第１受信手段と利用手段とを備え、前記第１出力手段は、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを前記楕円曲線変換装置へ出力し、ここで、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、前記第２受信手段は、前記利用装置から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、元Ｇとを受信し、前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、元Ｇｔとを算出し、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値であり、前記第２出力手段は、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを前記利用装置へ出力し、前記第１受信手段は、前記出力されたパラメータａ’及びｂ’と、元Ｇｔとを受信し、前記利用手段は、素数ｐと、前記受信したパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポンイトとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行うことを特徴とする。

【００３７】

【発明の実施の形態】本発明に係る１つの実施の形態としての楕円曲線変換装置２００について、図を用いて説明する。

１．楕円曲線変換装置２００の構成

楕円曲線変換装置２００は、図２に示すように、パラメータ受信部２１０、変換係数取得部２２０、変換楕円曲線算出部２３０、パラメータ送出部２４０から構成される。

（パラメータ受信部２１０）パラメータ受信部２１０は、外部の装置から、楕円曲線のパラメータａ、ｂと、前記楕円曲線上の元Ｇと、素数ｐとを受信する。ここで、ｐは、１６０ビットの素数である。

【００３８】前記外部の装置には、公開鍵暗号を用いる暗号装置、復号装置、デジタル署名装置、デジタル署名検証装置、鍵共有装置などが含まれる。前記外部の装置は、公開鍵暗号の安全性の根拠として楕円曲線上の離散対数問題を用いており、前記楕円曲線を有している。ここで、有限体ＧＦ（ｐ）上の任意に構成される前記楕円

曲線は、Ｅ：ｙ＾２　＝　ｘ＾３　＋ａｘ＋ｂ　で示され、前記元Ｇは、前記楕円曲線の任意に構成され、

Ｇ＝（ｘ０，ｙ０）

で表される。

（変換係数取得部２２０）変換係数取得部２２０は、図３に示すように、関数Ｔ（ｉ）を有する。関数Ｔ（ｉ）は、ｉ＝０、１、２、３、４のとき、それぞれ、－３、１、－１、２、－２の値を有する。また、関数Ｔ（ｉ）は、ｉ＝５、６、７、８、９、１０、１１、・・・のとき、３、４、－４、５、－５、６、－６、・・・の値を有する。

【００３９】変換係数取得部２２０は、ｉ＝０から始めて、ｉの値を１ずつ加算しながら、

（式２４）　－２＾３１＋１≦Ｔ（ｉ）≦２＾３１－１

を満たし、かつ、

（式２５）　Ｔ（ｉ）＝ｔ＾４×ａ　（ｍｏｄ　ｐ）

となる変換係数ｔであって、有限体ＧＦ（ｐ）上の元である変換係数ｔを算出する。

【００４０】ここで、式２４は、Ｔ（ｉ）が３２ビット以下になるように取られることを示している。なお、関数Ｔ（ｉ）は、ｉ＝０のときに、－３の値を有しており、変換係数取得部２２０は、ｉ＝０から始めて、ｉの値を１ずつ加算しながら、関数Ｔ（ｉ）の値を参照するので、最初に－３の値が参照される。

【００４１】また、関数Ｔ（ｉ）は、ｉ＝０のときに、－３の値を有していることを除いて、絶対値の小さい値から大きい値へと順に値を有しているので、絶対値の小さい値から順に参照することができる。（変換楕円曲線算出部２３０）変換楕円曲線算出部２３０は、有限体ＧＦ（ｐ）上に構成される変換楕円曲線Ｅｔ：ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’のパラメータａ’、ｂ’をそれぞれ次のようにして、算出する。

（式２６）　ａ’＝ａ×ｔ＾４

（式２７）　ｂ’＝ｂ×ｔ＾６

また、変換楕円曲線算出部２３０は、元Ｇに対応する変換楕円曲線Ｅｔ上の元Ｇｔ＝（ｘｔ０，ｙｔ０）を次のようにして、算出する。

（式２８）　ｘｔ０＝ｔ＾２×ｘ０

（式２９）　ｙｔ０＝ｔ＾３×ｙ０

なお、楕円曲線Ｅ上の任意の点は、以上のようにして生成されたパラメータａ’、ｂ’で定まる変換楕円曲線Ｅｔ上の１点に変換される。

（パラメータ送出部２４０）パラメータ送出部２４０は、前記算出された変換楕円曲線Ｅｔのパラメータａ’、ｂ’と、元Ｇｔ（ｘｔ０，ｙｔ０）とを前記外部の装置へ送出する。

２．楕円曲線変換装置２００の動作

（楕円曲線変換装置２００の全体の動作）楕円曲線変換装置２００の全体の動作について、図４に示すフローチャートを用いて、説明する。

【００４２】パラメータ受信部２１０は、外部の装置から素数ｐと、楕円曲線Ｅのパラメータａ及びｂとを受け取り（ステップＳ３０１）、前記楕円曲線上の元Ｇを受け取る（ステップＳ３０２）。次に、変換係数取得部２２０は、変換係数ｔを算出し（ステップＳ３０３）、変換楕円曲線算出部２３０は、有限体ＧＦ（ｐ）上に構成される変換楕円曲線Ｅｔのパラメータａ’、ｂ’と、元Ｇに対応する変換楕円曲線Ｅｔ上の元Ｇｔ＝（ｘｔ０，ｙｔ０）を算出し（ステップＳ３０４）、パラメータ送出部２４０は、前記算出された変換楕円曲線Ｅｔのパラメータａ’、ｂ’と、元Ｇｔ（ｘｔ０，ｙｔ０）とを前記外部の装置へ送出する（ステップＳ３０５）。

（変換係数取得部２２０の動作）次に、変換係数取得部２２０の動作について、図５に示すフローチャートを用いて説明する。

【００４３】変換係数取得部２２０は、ｉに０の値を設定する（ステップＳ３１１）。次に、変換係数取得部２２０は、関数Ｔ（ｉ）について、

－２＾３１＋１≦Ｔ（ｉ）≦２＾３１－１

を満たすかどうかを判定し、満たさないならば（ステップＳ３１２）、処理を終了する。満たすならば（ステップＳ３１２）、

Ｔ（ｉ）＝ｔ＾４×ａ　（ｍｏｄ　ｐ）

となる変換係数ｔを算出し（ステップＳ３１３）、算出された変換係数ｔが有限体ＧＦ（ｐ）上の元であるかどうかを判定し、有限体ＧＦ（ｐ）上の元であるなら（ステップＳ３１４）、処理を終了する。有限体ＧＦ（ｐ）上の元でないなら（ステップＳ３１４）、ｉに１を加算し（ステップＳ３１５）、再度ステップＳ３１２へ制御を戻す。

（変換楕円曲線算出部２３０の動作）次に、変換楕円曲線算出部２３０の動作について、図６に示すフローチャートを用いて説明する。

【００４４】変換楕円曲線算出部２３０は、有限体ＧＦ（ｐ）上に構成される変換楕円曲線Ｅｔのパラメータａ’＝ａ×ｔ＾４を算出し（ステップＳ３２１）、パラメータｂ’＝ｂ×ｔ＾６を算出する（ステップＳ３２２）。また、変換楕円曲線算出部２３０は、元Ｇに対応する変換楕円曲線Ｅｔ上の元Ｇｔ＝（ｘｔ０，ｙｔ０）として、ｘｔ０＝ｔ＾２×ｘ０を算出し（ステップＳ３２３）、ｙｔ０＝ｔ＾３×ｙ０を算出する（ステップＳ３２４）。

３．変換楕円曲線Ｅｔと楕円曲線Ｅとが同型である証明

ここでは、変換楕円曲線Ｅｔ：ｙ’＾２＝ｘ’＾３＋ａ×ｔ＾４×ｘ’＋ｂ×ｔ＾６と、楕円曲線Ｅ：ｙ＾２＝ｘ＾３＋ａ×ｘ＋ｂとが同型であることを証明する。なお、以下において、楕円曲線上の演算は、アフィン座標のものを取り扱う。

【００４５】楕円曲線Ｅ上の任意の点Ｐ（ｘ０，ｙ０）を取る。このとき、点Ｐは、Ｅ上の点であるから、

（式３０）　ｙ０＾２＝ｘ０＾３＋ａ×ｘ０＋ｂ

を満たしている。この変換により、点Ｐは、点Ｐ’（ｘ０’，ｙ０’）＝（ｔ＾２×ｘ０，ｔ＾３×ｙ０）に変換される。

【００４６】ここで、式３０の両辺に、ｔ＾６をかけると、

ｔ＾６×ｙ０＾２＝ｔ＾６×ｘ０＾３＋ｔ＾６×ａ×ｘ０＋ｔ＾６×ｂ

が得られる。この式は、次のように変形できる。

（ｔ＾３×ｙ０）＾２＝（ｔ＾２×ｘ０）＾３＋ａ×ｔ＾４×（ｔ＾２×ｘ０）＋ｂ×ｔ＾６

この式は、さらに、次のように変形できる。

【００４７】ｙ０’＾２＝ｘ０’＾３＋ａ×ｔ＾４×ｘ０’＋ｂ×ｔ＾６

これは、点Ｐ’が、変換楕円曲線Ｅｔ上にあることを示している。また、楕円曲線Ｅ上の点から変換楕円曲線Ｅｔ上の点への変換は、

（ｘ，ｙ）→（ｘ’，ｙ’）＝（ｔ＾２×ｘ，ｔ＾３×ｙ）

により示される。ここで、ｔ≠０であるので、以下に示す変換楕円曲線Ｅｔ上の点から楕円曲線Ｅ上への点の変換は、上記変換の逆変換であることは容易に分かる。

【００４８】（ｘ’，ｙ’）→（ｘ，ｙ）＝（ｘ’／（ｔ＾２），ｙ’／（ｔ＾３））

以上のことから、楕円曲線Ｅ上の点と変換楕円曲線Ｅｔ上の点とは、１対１に対応していることが分かる。次に、楕円曲線Ｅ上の任意の異なる２点Ｐ＝（ｘ１，ｙ１）、Ｑ＝（ｘ２，ｙ２）を取り、Ｒ＝Ｐ＋Ｑとし、Ｒの座標を（ｘ３，ｙ３）とする。このとき、前に述べたように、

＊ｘ３＝｛（ｙ２－ｙ１）／（ｘ２－ｘ１）｝＾２－ｘ１－ｘ２

ｙ３＝｛（ｙ２－ｙ１）／（ｘ２－ｘ１）｝（ｘ１－ｘ３）－ｙ１

となる。

【００４９】次に、本発明で用いた楕円曲線の変換により、楕円曲線Ｅ上の点Ｐ、点Ｑ、点Ｒが、それぞれ、変換楕円曲線Ｅｔ上の点Ｐ’、点Ｑ’、点Ｒ’に変換されるものとする。ここで、点Ｐ’、点Ｑ’、点Ｒ’の座標をそれぞれ、（ｘ１’，ｙ１’）、（ｘ２’，ｙ２’）、（ｘ３’，ｙ３’）とする。このとき、

ｘ１’＝ｔ＾２×ｘ１
ｙ１’＝ｔ＾３×ｙ１
ｘ２’＝ｔ＾２×ｘ２
ｙ２’＝ｔ＾３×ｙ２
ｘ３’＝ｔ＾２×ｘ３
ｙ３’＝ｔ＾３×ｙ３

が成り立つ。

【００５０】また、Ｒ”＝Ｐ’＋Ｑ’とする。ただし、ここにおける加算演算は、変換楕円曲線Ｅｔ上の加算を示す。Ｒ”の座標を（ｘ３”，ｙ３”）とすると、

ｘ３”＝｛（ｙ２’－ｙ１’）／（ｘ２’－ｘ１’）｝＾２－ｘ１’－ｘ２’

ｙ３”＝｛（ｙ２’－ｙ１’）／（ｘ２’－ｘ１’）｝（ｘ１’－ｘ３’）－ｙ１’

となる。

【００５１】ここで、この式におけるｘ１’、ｙ１’、ｘ２’、ｙ２’を、それぞれ、上記のように、ｘ１、ｙ１、ｘ２、ｙ２を用いて表すと、

ｘ３”＝｛（ｔ＾３×ｙ２－ｔ＾３×ｙ１）／（ｔ＾２×ｘ２－ｔ＾２×ｘ１）｝＾２－ｔ＾２×ｘ１－ｔ＾２×ｘ２
　＝｛ｔ（ｙ２－ｙ１）／（ｘ２－ｘ１）｝＾２－ｔ＾２×ｘ１－ｔ＾２×ｘ２
　＝ｔ＾２×｛｛（ｙ２－ｙ１）／（ｘ２－ｘ１）｝＾２－ｘ１－ｘ２｝
　＝ｔ＾２×ｘ３
　＝ｘ３’

ｙ３”＝｛（ｔ＾３×ｙ２－ｔ＾３×ｙ１）／（ｔ＾２×ｘ２－ｔ＾２×ｘ１）｝×（ｔ＾２×ｘ１－ｔ＾２×ｘ３）－ｔ＾３×ｙ１
　＝｛ｔ（ｙ２－ｙ１）／（ｘ２－ｘ１）｝×ｔ＾２（ｘ１－ｘ３）－ｔ＾３×ｙ１
　＝ｔ＾３×｛｛（ｙ２－ｙ１）／（ｘ２－ｘ１）｝×（ｘ１－ｘ３）－ｙ１｝
　＝ｔ＾３×ｙ３
　＝ｙ３’

となる。従って、Ｒ’とＲ”とは、等しい点を表していることが分かる。

【００５２】以上により、楕円曲線上の加算演算は、本変換においても、保存されることが分かる。次に、Ｑ＝Ｐの場合について、すなわち、２倍公式について、述べる。前と同様に、楕円曲線Ｅ上の任意の点Ｐに対して、Ｒ＝Ｐ＋Ｐとし、本発明で用いた楕円曲線の変換により、楕円曲線Ｅ上の点Ｐ、点Ｒが、それぞれ、変換楕円曲線

曲線Etの点P'、点R'に変換されるものとする。ここで、点P、点R、点P'、点R'の座標をそれぞれ、(x1, y1)、(x3, y3)、(x1', y1')、(x3', y3')とする。このとき、

$$x1' = t^2 \times x1$$
$$y1' = t^3 \times y1$$
$$x3' = t^2 \times x3$$
$$y3' = t^3 \times y3$$

が成り立つ。また、R"＝P'＋P'とする。＊

＊【0053】ただし、ここにおける2倍演算は、変換楕円曲線Et上の2倍演算を示す。点R"の座標を(x3", y3")とすると、

$$x3'' = \{(3 \times x1'^2 + a) / 2y1'\}^2 - 2x1'$$
$$y3'' = \{(3 \times x1'^2 + a) / 2y1'\}(x1' - x3') - y1'$$

となる。ここで、x1'、y1'をそれぞれ、x1、y1を用いて上記のように表すと、

$$
\begin{aligned}
x3'' &= \{\{(t^2 \times 3x1)^2 + a\} / (2 \times t^3 \times y1)\}^2 \\
&\quad - 2 \times t^2 \times x1 \\
&= t^2 \{(3x1^2 + a) / y1\}^2 - t^2 \times 2x1 \\
&= t^2 \{\{(3x1^2 + a) / y1\}^2 - 2x1\} \\
&= t^2 \times x3 \\
&= \{t(y2 - y1) / (x2 - x1)\}^2 - t^2 \times x1 \\
&\quad - t^2 \times x2 \\
&= t^2 \{\{(y2 - y1) / (x2 - x1)\}^2 \\
&\quad - x1 - x2\} \\
&= t^2 \times x3 \\
&= x3' \\
y3'' &= \{\{(t^2 \times 3x1)^2 + a\} / (2 \times t^3 \times y1)\} \\
&\quad \times (t^2 \times x1 - t^2 \times x3) - t^3 \times y1 \\
&= t^3 \{(3x1^2 + a) / 2y1\}(x1 - x3) \\
&\quad - t^3 \times y1 \\
&= t^3 \{\{(3x1^2 + a) / 2y1\}(x1 - x3) - y1\} \\
&= t^3 \times y3 \\
&= y3'
\end{aligned}
$$

となる。従って、R'とR"とは、等しい点を表していることが分かる。

【0054】以上により、楕円曲線上の2倍演算は、本変換においても、保存されることが分かる。以上に述べたことにより、楕円曲線Eと、本発明において用いる変換により生成された変換楕円曲線Etとは、同型であることが証明できた。

4．変換楕円曲線Etを用いる場合の計算量の評価

上記の実施の形態によると、変換楕円曲線Etのパラメータa'は、32ビット以下になるように取られるので、式18の計算量は、3Sqとなる。従って、楕円曲線上の加算の計算量は、12Mul＋4Sqとなり、2倍算の計算量は、3Mul＋6Sqとなる。このように、楕円曲線Eのパラメータaが、160ビットに近い値である場合とと比較すると2倍算において、1Mul分の計算量が削減できることが分かる。

【0055】上記に述べたように、関数T(i)は、i＝0のときに、－3の値を有していることを除いて、絶対値の小さい値から大きい値へと順に値を有しており、絶対値の小さい値から順に参照することができるので、より計算量の少ない変換楕円曲線から順に、適切な変換楕円曲線を選んでいくことができる。また、上記の実施の形態によると、変換楕円曲線Etのパラメータa'が、－3の場合、式18は、

$$
\begin{aligned}
M &= 3 \times X1^2 + a' \times Z1^4 \\
&= 3 \times X1^2 - 3 \times Z1^4 \\
&= 3 \times (X1 + Z1^2) \times (X1 - Z1^2)
\end{aligned}
$$

と変形できる。

【0056】最後の式において、計算量は、1Mul＋1Sqとなる。従って、楕円曲線上の加算の計算量は、12Mul＋4Sqとなり、2倍算の計算量は、4Mul＋4Sqとなる。このように、従来と比較すると2倍算において、2Sq分の計算量が削減できることが分かる。上記に述べたように、関数T(i)は、i＝0のときに、－3の値を有しており、変換係数取得部220は、i＝0から始めて、iの値を1ずつ加算しながら、関数T(i)の値を参照するので、最初に－3の値が参照される。従って、2倍算において、従来との比較で2Sq分の計算量が削減できる場合が、最初に検証されるので、最も適切な変換楕円曲線を1回で検出できる可能性がある。

【0057】このため、本実施の形態に示す変換楕円曲線を用いると、楕円曲線上の計算を高速化することができる。

5．変形例

変換係数取得部220は、次のようにして、変換係数t

を決定してもよい。変換係数取得部２２０は、乱数発生部を備えており、前記乱数発生部は、有限体ＧＦ（ｐ）上の元ｕ（$u \neq 0$）をランダムに発生する。次に、変換係数取得部２２０は、元ｕが、

（式３１）　$-2^{31}+1 \leqq u^4 \times a \pmod{p} \leqq 2^{31}-1$

を満たすかどうかを判定する。元ｕが式３１を満たすと判定された場合は、元ｕを変換係数ｔとして採用する。元ｕが式３１を満たさないと判定された場合は、再度、前記乱数発生部は、ランダムに元ｕを発生し、変換係数取得部２２０は、元ｕが、式３１を満たすかどうかを判定する。

【００５８】変換係数取得部２２０は、式３１を満たす元ｕが見つかるまで、前記乱数発生部による元ｕの発生と式３１を満たすかどうかの判定を繰り返す。また、変換係数取得部２２０は、式３１の代わりに、

（式３２）　$u^4 \times a \pmod{p} = -3$

を用いるとしてもよい。

６．楕円曲線変換装置２００の適用例

上記に説明した楕円曲線変換装置２００を適用する鍵共有システムを図７に示すシーケンス図を用いて説明する。

【００５９】ユーザＡ４５０、管理センタ４６０及びユーザＢ４７０は、ネットワークで接続されている。

（１）管理センタ４６０による楕円曲線の選択

管理センタ４６０は、素数ｐを選択し、有限体ＧＦ（ｐ）上の楕円曲線Ｅを選択し、Ｅのベースポイントを Ｇとし、Ｅの位数をｑとする（ステップＳ４１１）。つまり、ｑは、

（式２）　$q*G=0$

を満たす最小の正整数である。

【００６０】ここで、$E: y^2 = x^3 + a \times x + b$ であり、$G=(x0, y0)$ である。次に、管理センタ４６０は、ｐ、Ｅ、Ｇを楕円曲線変換装置２００へ送出する（ステップＳ４１２）。

【００６１】（２）楕円曲線変換装置２００による変換楕円曲線の生成

楕円曲線変換装置２００は、変換楕円曲線Ｅｔを算出し、元Ｇｔを算出する（ステップＳ４２１）。ここで、

$Et: y'^2 = x'^3 + a' \times x' + b'$、

$a' = a \times t^4$、

$b' = b \times t^6$、

$Gt = (xt0, yt0)$、

$xt0 = t^2 \times x0$、

$yt0 = t^3 \times y0$ である。

【００６２】次に、楕円曲線変換装置２００は、Ｅｔ、Ｇｔを管理センタ４６０へ送出する（ステップＳ４２２）。管理センタ４６０は、Ｐ、Ｅｔ、Ｇｔを各ユーザへ送出する（ステップＳ４１３）。

（３）ユーザによる秘密鍵の設定と公開鍵の生成

ユーザＡ４５０は、秘密鍵ｘＡを設定し（ステップＳ４０１）、ユーザＢ４７０は、秘密鍵ｘＢを設定する（ステップＳ４３１）。

【００６３】ユーザＡ４５０は、次式により、公開鍵ＹＡを算出し（ステップＳ４０２）、公開鍵ＹＡをユーザＢ４７０へ送出する（ステップＳ４０３）。

$YA = xA * Gt$

また、ユーザＢ４７０は、次式により、公開鍵ＹＢを算出し（ステップＳ４３２）、公開鍵ＹＢをユーザＡ４５０へ送出する（ステップＳ４３３）。

【００６４】$YB = xB * Gt$

（４）各ユーザによる共有鍵の生成

ユーザＡ４５０は、共有鍵をｘＡ＊ＹＢにより算出する（ステップＳ４０４）。また、ユーザＢ４７０は、共有鍵をｘＢ＊ＹＡにより算出する（ステップＳ４３４）。

【００６５】ここで、ユーザＡ４５０により算出された共有鍵ｘＡ＊ＹＢは、

$xA * YB = (xA \times xB) * Gt$

のように変形できる。また、ユーザＢ４７０により算出された共有鍵ｘＢ＊ＹＡは、

$$
\begin{aligned}
xB * YA &= (xB \times xA) * Gt \\
&= (xA \times xB) * Gt
\end{aligned}
$$

のように変形できる。

【００６６】従って、ユーザＡ４５０により算出された共有鍵ｘＡ＊ＹＢと、ユーザＢ４７０により算出された共有鍵ｘＢ＊ＹＡとが同じものであることは、明らかである。７．その他の変形例別の実施の形態の一つは、上記により示される楕円曲線変換方法であるとしてもよい。前記楕円曲線変換方法をコンピュータに実行させる楕円曲線変換プログラムを含むコンピュータ読み取り可能な記録媒体としてもよい。さらに、前記楕円曲線変換プログラムを通信回線を介して伝送するとしてもよい。

【００６７】また、上記に説明した楕円曲線変換装置を、暗号装置、復号装置、又は暗号装置と復号装置とからなる暗号システムに適用してもよい。また、上記に説明した楕円曲線変換装置を、デジタル署名装置、デジタル署名検証装置、又はデジタル署名装置とデジタル署名検証装置とからなるデジタル署名システムに適用してもよい。

【００６８】また、暗号装置、復号装置、デジタル署名装置、デジタル署名検証装置、又は鍵共有装置は、楕円曲線変換装置により算出された楕円曲線のパラメータａ’、ｂ’と元Ｇｔとを予め記憶しており、記憶している楕円曲線のパラメータａ’、ｂ’と元Ｇｔとを用いて、暗号、復号、デジタル署名、デジタル署名検証、又は鍵共有を行うとしてもよい。

【００６９】また、上記に示す実施の形態及びその複数の変形例を組み合わせてもよい。

【００７０】

【発明の効果】本発明は、１つの楕円曲線Ｅを変換して

他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置であって、外部から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポンイトとしての元Ｇとを受信する手段であって、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表される受信手段と、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得する手段であって、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満たす変換係数取得手段と、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイント元Ｇｔとを算出する手段であって、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値である楕円曲線算出手段と、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを外部へ出力する出力手段とを備える。

【００７１】この構成によると、ランダムに構成された楕円曲線と同じ安全性を有し、利用装置において高速な演算を可能にする楕円曲線を提供することができ、その実用的価値は非常に大きい。ここで、ｐは、１６０ビットの素数であり、前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が３２ビット以下の数になる、という条件を満たす変換係数ｔを取得するとしてもよい。

【００７２】この楕円曲線変換装置により変換された楕円曲線を利用装置において用いると、楕円曲線上の２倍算において、変換前の楕円曲線のパラメータａが、１６０ビットに近い値を取る場合と比較して、１Ｍｕｌ分の計算量が削減できることが分かる。ここで、前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が－３となる、という条件を満たす変換係数ｔを取得するとしてもよい。

【００７３】この楕円曲線変換装置により変換された楕円曲線を利用装置において用いると、楕円曲線上の２倍算において、従来と比較して、２Ｓｑ分の計算量が削減できることが分かる。ここで、前記変換係数取得手段は、変数Ｔとして、初期値を－３とし、初期値以外の値については、桁数の小さい値から大きい値へ順に取ることと、Ｔ＝ｔ＾４×ａ　（ｍｏｄ　ｐ）という条件を満たすかどうかを判定することとを繰り返すことにより、変換係数ｔを取得するとしてもよい。

【００７４】この構成によると、関数Ｔ（ｉ）は、ｉ＝０のときに、－３の値を有しており、変換係数取得部２２０は、ｉ＝０から始めて、ｉの値を１ずつ加算しながら、関数Ｔ（ｉ）の値を参照するので、最初に－３の値が参照される。従って、２倍算において、従来との比較で２Ｓｑ分の計算量が削減できる場合が、最初に検証されるので、最も適切な変換楕円曲線を１回で検出できる可能性がある。また、関数Ｔ（ｉ）は、ｉ＝０のときに、－３の値を有していることを除いて、絶対値の小さい値から大きい値へと順に値を有しており、絶対値の小さい値から順に参照することができるので、より計算量の少ない変換楕円曲線から順に、適切な変換楕円曲線を選んでいくことができる。

【００７５】また、本発明は、１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置と、生成された楕円曲線Ｅｔを利用する利用装置とからなる楕円曲線利用システムであって、前記利用装置は、第１出力手段と第１受信手段と利用手段とを備え、前記楕円曲線変換装置は、第２受信手段と変換係数取得手段と楕円曲線算出手段と第２出力手段とを備え、前記第１出力手段は、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを前記楕円曲線変換装置へ出力し、ここで、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、前記第２受信手段は、前記利用装置から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、元Ｇとを受信し、前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出し、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値であり、前記第２出力手段は、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを前記利用装置へ出力し、前記第１受信手段は、前記出力されたパラメータａ’及びｂ’と、元Ｇｔとを受信し、前記利用手段は、素数ｐと、前記受信したパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポイントとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行う。

【００７６】この構成によると、ランダムに構成された楕円曲線と同じ安全性を有し、高速な演算を可能にする楕円曲線を利用することができ、その実用的価値は非常に大きい。ここで、ｐは、１６０ビットの素数であり、前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が３２ビット以下の数になる、という条件を満たす変換

係数ｔを取得するとしてもよい。

【００７７】この構成によると、変換された楕円曲線を用いるので、楕円曲線上の２倍算において、変換前の楕円曲線のパラメータａが、１６０ビットに近い値を取る場合と比較して、１Ｍｕｌ分の計算量が削減できることが分かる。ここで、前記変換係数取得手段は、ｔ＾４×ａ　（ｍｏｄ　ｐ）が－３となる、という条件を満たす変換係数ｔを取得するとしてもよい。

【００７８】この構成によると、変換された楕円曲線を用いるので、楕円曲線上の２倍算において、従来と比較して、２Ｓｑ分の計算量が削減できることが分かる。ここで、前記変換係数取得手段は、変数Ｔとして、初期値を－３とし、初期値以外の値については、桁数の小さい値から大きい値へ順に取ることと、Ｔ＝ｔ＾４×ａ　（ｍｏｄ　ｐ）という条件を満たすかどうかを判定することとを繰り返すことにより、変換係数ｔを取得するとしてもよい。

【００７９】この構成によると、関数Ｔ（ｉ）は、ｉ＝０のときに、－３の値を有しており、変換係数取得部２２０は、ｉ＝０から始めて、ｉの値を１ずつ加算しながら、関数Ｔ（ｉ）の値を参照するので、最初に－３の値が参照される。従って、２倍算において、従来との比較で２Ｓｑ分の計算量が削減できる場合が、最初に検証されるので、最も適切な変換楕円曲線を１回で検出できる可能性がある。また、関数Ｔ（ｉ）は、ｉ＝０のときに、－３の値を有していることを除いて、絶対値の小さい値から大きい値へと順に値を有しており、絶対値の小さい値から順に参照することができるので、より計算量の少ない変換楕円曲線から順に、適切な変換楕円曲線を選んでいくことができる。

【００８０】また、本発明は、第２受信手段と変換係数取得手段と楕円曲線算出手段と第２出力手段とを備え、１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換装置から、前記生成された楕円曲線Ｅｔを受信して利用する利用装置であって、前記利用装置は、第１出力手段と第１受信手段と利用手段とを備え、前記第１出力手段は、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを前記楕円曲線変換装置へ出力し、ここで、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、前記第２受信手段は、前記利用装置から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、元Ｇとを受信し、前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、元Ｇｔとを算出し、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値であり、前記第２出力手段は、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを前記利用装置へ出力し、前記第１受信手段は、前記出力されたパラメータａ’及びｂ’と、元Ｇｔとを受信し、前記利用手段は、素数ｐと、前記受信したパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポンイトとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行う。

【００８１】この構成によると、ランダムに構成された楕円曲線と同じ安全性を有し、高速な演算を可能にする楕円曲線を利用することができ、その実用的価値は非常に大きい。また、本発明は、１つの楕円曲線Ｅを変換して生成された楕円曲線Ｅｔを利用する利用装置であって、前記利用装置は、楕円曲線Ｅｔのパラメータａ’及びｂ’と、ベースポイントとしての元Ｇｔとを記憶している記憶手段と、ｐと、前記記憶しているパラメータａ’及びｂ’とで定まる楕円曲線と、ベースポイントとしての元Ｇｔとを用いて、有限体ＧＦ（ｐ）上で定義される楕円曲線上での演算に基づき、離散対数問題を安全性の根拠とする暗号、復号、デジタル署名、デジタル署名検証又は鍵共有を行う利用手段とを備え、ここで、パラメータａ’及びｂ’と、元Ｇｔとは楕円曲線変換装置により生成され、前記楕円曲線変換装置は、変換係数取得手段、楕円曲線算出手段を備え、ｐは素数であり、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、ベースポンイトとしての元Ｇが、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表され、前記変換係数取得手段は、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得し、ここで、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満し、前記楕円曲線算出手段は、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出し、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、ここで、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝　ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値である。

【００８２】この構成によると、ランダムに構成された楕円曲線と同じ安全性を有し、高速な演算を可能にする楕円曲線を利用することができ、その実用的価値は非常に大きい。また、本発明は、１つの楕円曲線Ｅを変換し

て他の１つの楕円曲線Ｅｔを生成する楕円曲線変換方法であって、外部から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポンイトとしての元Ｇとを受信するステップであって、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表される受信ステップと、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得するステップであって、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満たす変換係数算出ステップと、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出するステップであって、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値である楕円曲線算出ステップと、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを外部へ出力する出力ステップとを含む。

【００８３】この方法を用いると、ランダムに構成された楕円曲線と同じ安全性を有し、利用装置において高速な演算を可能にする楕円曲線を生成することができ、その実用的価値は非常に大きい。また、本発明は、１つの楕円曲線Ｅを変換して他の１つの楕円曲線Ｅｔを生成する楕円曲線変換プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、前記プログラムは、外部から、素数ｐと、楕円曲線Ｅのパラメータａ及びパラメータｂと、ベースポイントとしての元Ｇとを受信するステップであって、楕円曲線Ｅは、有限体ＧＦ（ｐ）上で定義され、ｙ＾２＝ｘ＾３＋ａｘ＋ｂで表され、元Ｇは、楕円曲線Ｅ上に存在し、Ｇ＝（ｘ０，ｙ０）で表される受信ステップと、有限体ＧＦ（ｐ）上に存在する変換係数ｔを取得するステップであって、変換係数ｔは、ｔ≠０であり、かつ、ｔ＾４×ａ　（ｍｏｄ　ｐ）は、素数ｐと比較して桁数が小さい、という条件を満たす変換係数算出ステップと、前記取得された変換係数ｔを用いて、次式により、楕円曲線Ｅｔのパラメータａ’及びｂ’と、新たなベースポイントとしての元Ｇｔとを算出するステップであって、ａ’＝ａ×ｔ＾４、ｂ’＝ｂ×ｔ＾６、ｘｔ０＝ｔ＾２×ｘ０、ｙｔ０＝ｔ＾３×ｙ０、楕円曲線Ｅｔは、有限体ＧＦ（ｐ）上で定義され、ｙ’＾２　＝ｘ’＾３　＋ａ’×ｘ’＋ｂ’で表され、ｘｔ０、ｙｔ０は、それぞれ元Ｇｔのｘ座標値、ｙ座標値である楕円曲線算出ステップと、前記算出されたパラメータａ’及びｂ’と、元Ｇｔとを外部へ出力する出力ステップとを含む。

【００８４】この媒体に記録されているプログラムをコンピュータで実行することにより、ランダムに構成された楕円曲線と同じ安全性を有し、利用装置において高速な演算を可能にする楕円曲線を生成することができ、その実用的価値は非常に大きい。

【図面の簡単な説明】

【図１】エルガマル署名によるデジタル署名方式の手順を示すシーケンス図である。

【図２】本発明に係る１つの実施の形態としての楕円曲線変換装置のブロック図である。

【図３】図２に示す楕円曲線変換装置で用いられる関数Ｔ（ｉ）を説明する表である。

【図４】図２に示す楕円曲線変換装置の動作を示すフローチャートである。

【図５】図２に示す楕円曲線変換装置の変換係数取得部の動作を示すフローチャートである。

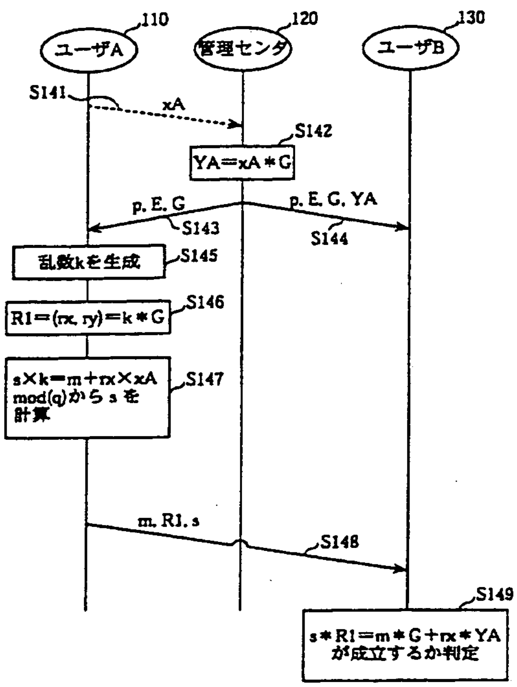
【図６】図２に示す楕円曲線変換装置の変換楕円曲線算出部の動作を示すフローチャートである。

【図７】図２に示す楕円曲線変換装置を適用する鍵共有システムの動作手順を示すシーケンス図である。

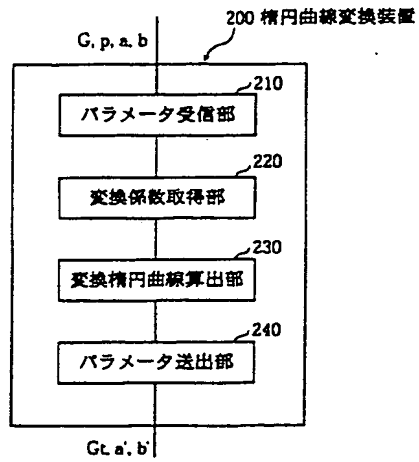
【符号の説明】

２００　楕円曲線変換装置
２１０　パラメータ受信部
２２０　変換係数取得部
２３０　変換楕円曲線算出部
２４０　パラメータ送出部

【図１】



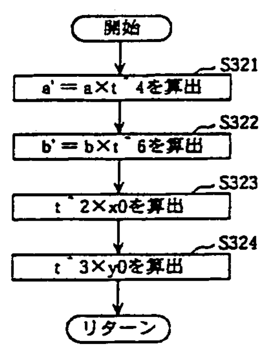
【図２】



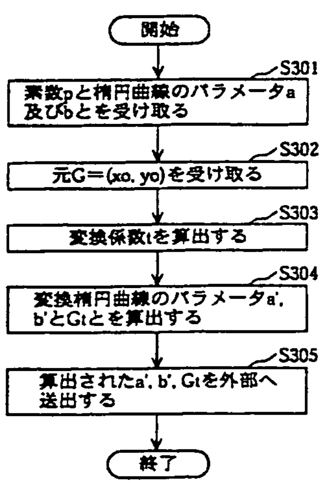
【図３】

i	T(i)
0	−3
1	1
2	−1
3	2
4	−2
5	3
6	4
7	−4
8	5
9	−5
10	6
11	−6
⋮	⋮

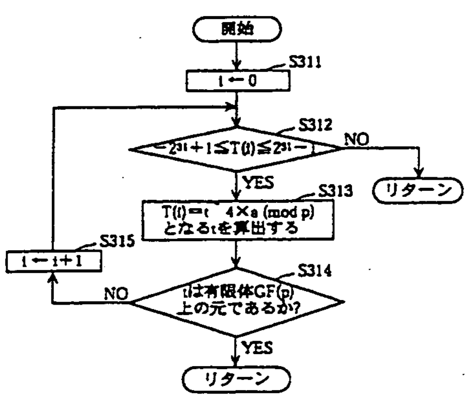
【図６】



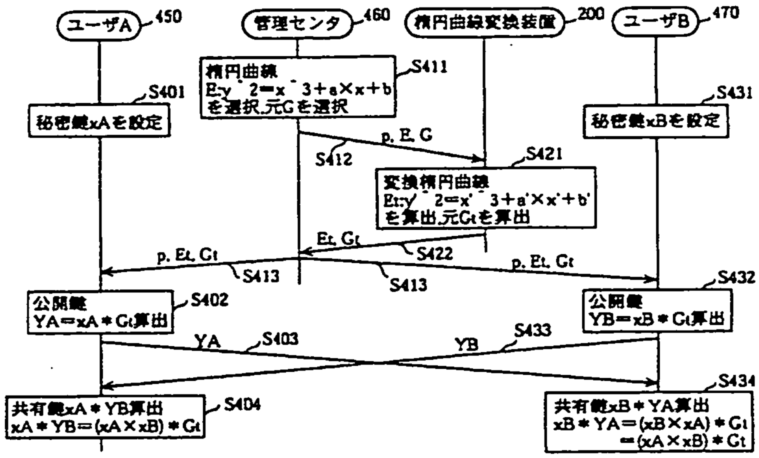
【図４】



【図５】



【図７】


ユーザA 450
管理センタ 460
楕円曲線変換装置 200
ユーザB 470
S411
楕円曲線
E:y^2=x^3+a×x+b
を選択,元Gを選択
S401
秘密鍵xAを設定
S431
秘密鍵xBを設定
p, E, G
S412
S421
変換楕円曲線
Et:y'^2=x'^3+a'×x'+b'
を算出,元Gtを算出
Et, Gt
S422
p, Et, Gt
S413
S413
p, Et, Gt
S402
公開鍵
YA=xA＊Gt算出
S432
公開鍵
YB=xB＊Gt算出
YA
S403
YB
S433
S404
共有鍵xA＊YB算出
xA＊YB=(xA×xB)＊Gt
S434
共有鍵xB＊YA算出
xB＊YA=(xB×xA)＊Gt
=(xA×xB)＊Gt